UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/720,085	12/20/2000	Louis Goubin	T2146-906752	6949

181 7590 05/15/2007

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
TO, BAOTRAN N	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
05/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/720,085	GOUBIN ET AL.	
	Examiner	Art Unit	
	Baotran N. To	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/01/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14 and 17-34* is/are rejected.

7)☒ Claim(s) *15 and 16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Docketing

1. Please note that the application has been re-docketed to a different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the Office action.

This Office action is responsive to the Applicant's Amendment filed 03/01/2007.

Claims 14, 16, and 17 are amended.

Claims 14-34 are pending.

Response to Arguments

2. Applicant's arguments filed 03/01/2007 have been fully considered but they are not persuasive.

Applicant argues that Kocher does not teach or suggest at least this feature of claim 14 "without any division operation at the level of the smart card" (page 1 of Remarks).

Examiner respectfully disagrees with this argument. Kocher explicitly discloses calculating the M' at the prover and exchange the M' to the verifier for validation. The process is implementing the Montgomery reduction technique to do modular reduction without any division (i.e., Montgomery reduction is a technique which allows efficient implementation of modular multiplication without explicitly carrying out the classical

modular reduction step) (Col 17 lines 56-62). Thus, it is clear that Kocher discloses the feature "without any division operation at level of the smart card."

Applicant further argues, "Kocher also fails to teach or suggest an electronic communication means of the terminal transmitting to the smart card said response data comprising at least a prevalidation value, where the prevalidation value represents at least a quotient of a modulo n calculation, as recited in Claim 14 (page 2 of Remarks).

Examiner respectfully disagrees with the applicant. In figure 1, Kocher describes an authentication process between a token, (e.g. smart card), and a terminal, (e.g. server). The figure 1 shows clearly the computation process requires at each party. At step 160, the terminal calculates the value A' to authenticate with A came from the smart card. This A' is similar to M' in Col 17 lines 45, which includes a quotient of a modulo n calculation. And further, Figure 3 shows a process of authentication comprising a calculation process by transmitting information back and forth between two parties, wherein the output of R' (335) is transferred back to the sender for further process. Therefore, it is clear that Kocher teaches the feature of claim 14.

For at least the above reasons, it is believed that the rejection is maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –
(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 14 and 34 are rejected under 35 U.S.C. 102(e) as being anticipated by Kocher et al (U.S. Patent 6,304,658 B1) hereinafter Kocher.

As per claims 14 and 34, Kocher discloses a method for verifying either a signature or an authentication utilizing an asymmetric private-key and public-key (e, n) cryptographic calculation process between a terminal having first computing means provided with a first computing capacity and a smart card (i.e., leak-proof cryptography authentication method above utilizing smart card and a terminal such as servers) (Col 1 lines 40-45, Figure 1) comprising second computing means provided with second computing capacity lower than said first computing capacity" in (Col 15 lines 30-45), said terminal including electronic communication means for communicating with the smart card, wherein said first computing means of the terminal performs first cryptographic calculations with said private key (d) to respectively produce calculation of a signature value or an authentication value constituting response data (Col 15 lines 30-45, and Col 16 lines 28-52), and said second computing means of the smart card, based on said response data, performs second cryptographic calculations with said

public key to respectively perform said signature verification or said authentication (Col 15 lines 45-57), and the first and second cryptographic calculations serving to implement the calculation of modulo-n multiplications, wherein the cryptographic calculation process uses said public key comprising a public exponent e and a public modulo n, and said a private key comprising a private exponent (Col 15 lines 30-45, and Col 16 lines 28-52), said method further comprising:

using said first computing means to calculate at the level of said terminal at least one prevalidation value (i.e., m') representing at least a quotient of a modulo n calculation (m', Col 17 line 45, Col 16 lines 61-67, and Col 7 lines 30- 55);

using said electronic communication means of the terminal to transmit to the smart card said response data comprising at least said prevalidation value (Col 21 lines 20-34); and

retrieving said prevalidation value by the smart card and using said second computing means to perform at least one modular reduction by utilizing said prevalidation value to obtain the remainder of the modulo calculation (i.e., The decrypting process) (Col 16 lines 61-67, and Col 7 lines 30-55), without any division operation at the level of the smart card (i.e., Montgomery reduction is a technique which allows efficient implementation of modular multiplication without explicitly carrying out the classical modular reduction step) (Col 17 lines 56-62).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 17-18, 21-27, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Blind Signature Schemes, (Menezes et al, Handbook of Applied Cryptography, Chapter 11.8.1 Pg 475), hereinafter Menezes (Cited in PTO 892 dated 05/18/05), and further in view of Liskov et al, (U.S. Patent 6,411,715 B1), hereinafter Liskov (Cited in PTO 892 dated 09/08/04).

As per claim 17, however, the Quotient Q2 is not directly taught. Nevertheless, Q2 equation is formulated to R*(R*R-Q1*n)/n so that the result of the signature verification is equal to Zero. This verification method is common in art and also taught by the RSA (Col 2 lines 35-47). The verification process is concluded when the decrypted message is the same as the sent message or another word the difference of the messages equals to zero. In additional, the blind signature method is also implemented in the formulation of Q_2 (See Claim 15 basis of rejection using the blind Signature), where the equation is divided by n. Therefore, it would have been obvious for one having ordinary skill in the art at the time the invention was made to incorporate

the blind signature and the RSA signature verification method into Kocher's invention to reduce the processing burden on the Smart card processor which is limited.

As per claim 18, the blinding signature and the RSA signature verification method described in claims 15, 16 and 17 are also applied.

As per claims 21 and 22, Kocher discloses a method according to claims 16 and 18, characterized in that, for an authentication verification operation, said method further comprises the step for transmitting a prompt value from the smart card to the terminal (Col 15 lines 35-40). The prompt value in Col 15 lines 35-40 is the message M, which is not limited to the text message. The message must be originated from party B in order to verify the received message is the same as the original.

As per claims 23 and 24, Kocher discloses "a method according to claims 21 and 22, characterized in that said prompt value comprises a random value d modulo n, said response value M comprises an encrypted value B, and said function of the response value comprises a function f(A) of said random value d" (Col 15 lines 35-40).

As rejected in claims 21 and 22, the f(A) is recited as f(M) = Md mod n (Col 15 lines 35-40).

As per claims 25-27, Kocher discloses a method according to claims 16 and 21-22, characterized in that said function f(A) if said random value A comprises a function among the functions f(A)=A" in (Col 15 lines 35-40). The function taught is Md modn. If n = 1 and d=1, then f(A) = A. However, the "f(A)=n-A, f(A)= C*Amodn, f(A)= -C*A modn"

is not taught by Kocher. Nevertheless, the result of the f(A) is depending on a mathematical functions f (A mod n). Therefore it would have been obvious at the time of the invention was made for one having ordinary skill in the art to implement plurality of different mathematical functions to acquire different results to add more verification steps of the signature.

As per claims 31 and 32, Kocher discloses a method according to claim 23, characterized in that said function f(A) of said random value A is the function f(A)=A, which makes it possible to verify the equality of said difference and the validity of said authentication without any division operation for the modular reduction" in (Col 15 lines 35-40, and Col 17 lines 30-65). Montgomery's reduction is an arithmetic reduction performing without any division operation (Col 17 lines 60-65).

5. Claims 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Menezes, and further in view of Stinson, Cryptography theory and Practice, CRC Press, Inc. page 3, hereinafter Stinson (Cited in PTO 892 dated 09/08/04).

As per claims 28, 29, and 30, Kocher and Menezes do not clearly teach "a method according to claim 25, 26, and 27, respectively characterized in that at the level of the smart card, the calculation of said function f(A)=C*A mod n comprises calculation of the value C*A and storing of said value if C*A < n, and the calculation and storing of the value C*A –n if not, and in that calculation of said function f(A) = -C*A modulo n comprises calculation of the value n-C*A and storing of said value if n-C*A ≥ 0, and

otherwise calculation of the intermediate value C*n-C*A, and if said intermediate value is greater than or equal to zero, calculation and storing of the value of –C*A modulo n, for verifying the equality of said authentication without any division for the modular reduction". Nevertheless, the modular reduction method in the claim is the basic mathematic of modular reduction comprise of multiplication and subtraction only. The same method is explained in Stinson on page 3, (the definition 1.2). The C is similar to q1 and r1 is the remainder of a division of m by b. The checking of the difference less than or equal to 0 is to find out the arithmetic completed or not. Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to implement the modular reduction method without any division by trying number of variables until the remainder is found. The method would require minimal processing capacity given that n is not sufficiently large.

6. Claims 19 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Menezes, and further in view of Poore et al. (U.S. Patent 6,202,933 B1) hereinafter Poore (Cited in PTO 892 dated 09/08/04).

As per claims 19 and 20, Kocher and Menezes do not disclose, "the applying a condensation function to said message to obtain a message digest CM; and concatenating said message digest with a constant value." Nevertheless, the feature is taught clearly by Poore in(Col 4 lines 52-56). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify the

invention to include Poore's teaching so that the signature is further be verified by using its digest.

7. Claim 33 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Poore et al. (U.S. Patent 6,202,933 B1) hereinafter Poore (Cited in PTO 892 dated 09/08/04).

As per claim 33, the encrypted value B, and a quotient value Q in claims 14, 15, and 17 is incorporated. However, Kocher does not teach the concatenation of the two values. Nevertheless, it is taught in Poore in (Col 4 lines 52-56). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to combine Poore's teaching to add a security feature to the message transferring process.

Allowable Subject Matter

8. Claims 15 and 16 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

9. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

BT
05/08/2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100